

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT
(Under 37 CFR 1.97(b) or 1.97(c))

Docket No.
00001-0436

In Re Application Of: VANSTONE, Scott et al.

Serial No.
10/092,972

Filing Date
March 8, 2002

Examiner
Not Yet Assigned

Group Art Unit
2131

Title: **KEY AGREEMENT & TRANSPORT PROTOCOL**

RECEIVED

JUN 10 2002

Address to:
Assistant Commissioner for Patents
Washington, D.C. 20231

Technology Center 2100

37 CFR 1.97(b)

1. ☒ The Information Disclosure Statement submitted herewith is being filed within three months of the filing of a national application; within three months of the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; or before the mailing date of a first Office Action on the merits, whichever event occurs last.

37 CFR 1.97(c)

2. ☐ The Information Disclosure Statement submitted herewith is being filed after three months of the filing of a national application, or the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; or after the mailing date of a first Office Action on the merits, whichever occurred last but before the mailing date of either:

1. a Final Action under 37 CFR 1.113, or
 2. a Notice of Allowance under 37 CFR 1.311,
- whichever occurs first.

Also submitted herewith is:

- ☐ a certification as specified in 37 CFR 1.97(e);

OR

- ☐ the fee set forth in 37 CFR 1.17(p) for submission of an Information Disclosure Statement under 37 CFR 1.97(c).

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT
(Under 37 CFR 1.97(b) or 1.97(c))

Docket No.
00001-0436

In Re Application Of: VANSTONE, Scott et al.

Serial No.
10/092,972

Filing Date
March 8, 2002

Examiner
Not Yet Assigned

Group Art Unit
2131

Title: ~~OPEN~~ AGREEMENT & TRANSPORT PROTOCOL



Payment of Fee

(Only complete if Applicant elects to pay the fee set forth in 37 CFR 1.17(p))

- ☐ A check in the amount of _____ is attached.
- ☐ The Assistant Commissioner is hereby authorized to charge and credit Deposit Account No. _____ as described below. A duplicate copy of this sheet is enclosed.
- ☐ Charge the amount of _____
- ☐ Credit any overpayment.
- ☐ Charge any additional fee required.

RECEIVED

JUN 10 2002

Technology Center 2100

Certificate of Transmission by Facsimile*

I certify that this document and authorization to charge deposit account is being facsimile transmitted to the United States Patent and Trademark Office (Fax. No. _____)

_____ on _____
(Date)

Signature

Typed or Printed Name of Person Signing Certificate

*This certificate may only be used if paying by deposit account.

Certificate of Mailing by First Class Mail

I certify that this document and fee is being deposited on _____ with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

Dated: 3 June 02

Signature

John R.S. Orange
Orange & Chari
Suite 4900, P.O. Box 190
66 Wellington Street West
Toronto, Ontario
M5K 1H6
Canada

CC:

ATTORNEY DOCKET NO.: 00001-0436
CUSTOMER NUMBER: 27,155



IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re patent application of:

VANSTONE et al.

Serial No.: 10/092,972 Group Art Unit: 2131
Filed: 03/08/2002 Examiner: Not Yet Assigned
Title: **KEY AGREEMENT & TRANSPORT PROTOCOL**

Commissioner of Patents and Trademarks
Washington, D.C. 20231

RECEIVED

JUN 10 2002

Technology Center 2100

Dear Sir:

INFORMATION DISCLOSURE STATEMENT

Pursuant to the duty to disclose under 37 CFR §1.56, Applicant submits herewith a Form PTO/SB/08A listing references of which the Applicant is aware and which are brought to the attention of the Examiner. In accordance with 37 CFR §1.98(a)(2), a copy of each document listed in the enclosed Form PTO/SB/08A is submitted herewith.

Pursuant to 35 USC §120, this application relies on the earlier filing date(s) of the following prior application(s):

<u>Serial Number</u>	<u>Filing Date</u>
08/426,090	04/21/1995

The filing of this IDS shall not be construed as a representation that a search has been made, an admission that the information cited is, or is considered to be, material for patentability, or that no other material information exists. This filing shall not be construed as an admission against interest in any matter.

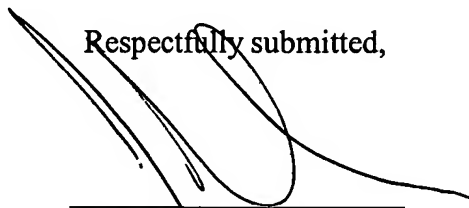
This IDS is submitted pursuant to 37 CFR §1.97(b) and, accordingly, no fee is believed to be due for consideration of the documents submitted herewith.

Applicant respectfully requests consideration of the items listed and requests the Examiner to return a copy of the attached Form PTO/SB/08A after being marked as being considered by the Examiner.

Date:

4 June 02

Respectfully submitted,



John R. S. Orange
Registration No. 29,725
Agent/Attorney for Applicant

Orange & Chari
Suite 4900, P.O. Box 190
66 Wellington Street West
Toronto, Ontario M5K 1H6, Canada

Tel: (416) 601-8440
Fax: (416) 601-8454

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known

Application Number	10/092,972
Filing Date	03-08-2002
First Named Inventor	VANSTONE
Group Art Unit	2131
Examiner Name	Not Yet Assigned
Attorney Docket Number	00001-0436

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials ¹	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
		BOYD, COLIN and MAO, WENBO, "Design and Analysis of Key Exchange Protocols via Secure Channel Identification", Advances in Cryptology - ASIACRYPT '94, 4th International Conference on the Theory and Applications of Cryptology, Proceedings, November 28 1994, Pages 171-181, Springer, Wollongong, Australia.	
		DIFFIE, WHITFIELD et al., "Authentication and Authenticated Key Exchanges," Designs, Codes and Cryptography, June 1992, Pages 107-125, Vol 2, No 32, Kluwer Academic Publishers, the Netherlands.	
		MATSUMOTO, "On Seeking Smart Public-Key-Distribution Systems", Transactions of the IECE of Japan, February 1986, Pages 99-106, Volume E69, No. 2.	
		HORSTER, "Meta-ElGamal Signature Schemes", 1994 2nd Association of Computing Machinery Computer and Communications Security Conference, May 31, 1994, Pages 96-107, ACM Press, Fairfax.	
		HORSTER, "Meta-Message Recovery and and Meta-Blind signature schemes based on the discrete logarithm problem and their applications", Advances in Cryptology, ASIACRYPT '94 (LNCS 917), Pages 224-237, Springer Verlag.	
		NYBERG, "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem", Advances in Cryptology, EUROCRYPT '94 pp. 182-193, Springer-Verlag.	

Examiner
Signature

Date
Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.